UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
8550 Commonwealth Ave., Apt. 415
Buena Park, California 90621

Case No. 8:18-MJ-00577

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2251(d), 2252A(a)(2), (a)(5)(B)	See attached affidavit

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Aron Klaff, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

Judge's signature

City and state: Santa Ana, California

Edward Infante, U.S. Magistrate Judge
Printed name and title

AUSA: Jake Nare, 714-338-3549

AFFIDAVIT

I, Aron Klaff, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI") since February 2009 and I am currently assigned to the HSI Orange County Child Exploitation Task Force ("OCCETF"). I have been assigned to OCCETF since January 2018. Prior to my employment with HSI, I completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia, in March 2003. From March 2003 to April 2004, I worked as a SA for the U.S. Department of Agriculture, Office of Inspector General. From April 2004 through February 2009, I worked as a SA for the U.S. Department of Labor, Office of Labor Racketeering and Fraud Investigations.

2. While employed by HSI as a SA, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, child pornography, internal employee misconduct, immigration fraud, money laundering, and the smuggling of illegal aliens. I have a working knowledge of, and have received training from other experienced agents and officers in, crimes involving child pornography and child exploitation. In my role as a SA for HSI, I have reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer engaged in

enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of an application for a warrant to search the premises located at 8550 Commonwealth Ave., Apt. 415, Buena Park, California 90621 (the "SUBJECT PREMISES"), more fully described below and in **Attachment A**, which is attached hereto and incorporated herein by reference, and to seize evidence, fruits, and instrumentalities of criminal conduct, as specified in **Attachment B**, which is also attached hereto and incorporated by reference, that is, violations of Title 18, United States Code, Sections 2251(d) (advertisement of child pornography), 2252A(a)(2) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography) (collectively, the "Subject Offenses").

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. PREMISES TO BE SEARCHED

5. The premises to be searched is the property located at 8550 Commonwealth Ave., Apt 415, Buena Park, California, 90621. The SUBJECT PREMISES is an apartment unit on the second story of a two-story multi-family apartment complex with the front door facing east. The exterior color of the apartment building is beige in color and has a dark brown front door. The front door has dull gold-colored numbers on it that read "415." While facing the front door, there is one rectangular aluminum window for Apt 415 to the right of the front door. Just below the window lies an air conditioning unit which is affixed onto the exterior wall of the building. The front of the apartment complex has a brown sign with off-white letters with the apartment complex's information as follows: Fullerton Court Apartment Homes (714) 670-1308, 8550 Commonwealth Ave.

IV. SUMMARY OF PROBABLE CAUSE

6. Along with other members of law enforcement, I have been investigating individuals who obtain, possess, view, and distribute child pornography. As set forth in greater detail below, law enforcement has identified a person with an online name of "Nick Johnson" and an email address of NicRob555@gmail.com, as being associated with the uploading and posting of at least 127 sexually explicit images of children to his online account along with hundreds of other pictures of child erotica. The computer was connected to the Internet using Internet Protocol ("IP") address 2602:304:cd8d:f1c0:4db2:5a99:91ce:e86e ("SUSPECT IP ADDRESS")

when the sexually explicit images were uploaded. SUSPECT IP ADDRESS is assigned to an Internet subscriber named David LEWIS ("LEWIS") at the SUBJECT PREMISES.

V. DEFINITIONS

7. The following definitions apply to this affidavit and **Attachment B**:

a. The terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined in 18 U.S.C. § 2256.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. The term "computer" is defined in 18 U.S.C. § 1030(e)(1).

d. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related

communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. The term "Internet" is defined as the worldwide network of computers – a noncommercial, self-governing network devoted mostly to communication and research with roughly 3.2 billion users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university,

employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

g. The term "Internet Protocol" ("IP") is defined as the primary protocol upon which the Internet is based. IP allows a packet of information to travel through multiple networks (groups of linked computers) on the way to its ultimate destination.

h. The term "IP address" is defined as a unique number assigned to each computer directly connected to the Internet (for example, 74.100.66.74). Each computer connected to the Internet is assigned a unique IP address while it is connected. The IP address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP address is only assigned for the duration of that online session.

i. The term "Internet Service Provider" ("ISP") is defined as a business that allows a user to dial into or link through its computers, thereby allowing the user to connect to the Internet for a fee. ISPs generally provide only an Internet connection, an electronic mail address, and maybe Internet browsing software. A user can also connect to the Internet through a commercial online service such as AT&T, Verizon, or Time Warner Cable. With this kind of connection, the user gets Internet access and the proprietary features offered by the online service, such as chat rooms and searchable databases.

j. "File Transfer Protocol" ("FTP") is a standard network protocol used to transfer computer files from one host

to another over a computer network, such as the Internet. FTP, built on client-server architecture, uses separate control and data connections between the client and the server.

k. A "hash value" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

l. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

n. A "website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

o. The term virtual private network ("VPN") is defined as a method of sending all of an Internet user's Internet traffic through a private, encrypted tunnel. The use of a VPN provides greater control of how a user is identified online. A VPN creates a virtual encrypted "tunnel" between an Internet user and a remote server operated by a VPN service. All external Internet traffic is routed through this tunnel, so that the Internet user's ISP cannot see the data being transmitted. The end result is that the Internet user's computer appears to have the IP address of the VPN server, masking the true identity of the Internet user. VPN's are used as a tool to protect the privacy of individuals and businesses, but are also widely used by criminals to disguise their true geographic location in order to evade identification by law enforcement.

VI. STATEMENT OF PROBABLE CAUSE

A. Cyber Tip Report ID# 29684450 from Google Sent to the National Center for Missing and Exploited Children (NCMEC)

8. On March 27, 2018, a representative of Google contacted the National Center for Missing and Exploited Children (NCMEC) regarding an allegation of child sexual exploitation. As a result, NCMEC generated Cyber Tipline Report, ID# 29684450. Google reported that one of its users, utilizing SUBJECT IP ADDRESS, posted child pornographic images to his Google account associated with the email address NicRob555@gmail.com. The report detailed 127 sexually explicit images of children that were uploaded by the user on dates between the timeframe

February 27, 2018 through March 23, 2018. On March 26, 2018, Google became aware of the reported content which was stored in Google Photos infrastructure.

B. Description of Two Uploaded Sexually Explicit Images

9. On or about October 9, 2018, I reviewed Cyber Tipline Report, ID# 29684450, which included 127 sexually explicit images depicting child pornography. Of the 127 images depicting child pornography, one of the images I reviewed depicted an adult male inserting his finger into the vagina of a nude female, who was approximately four to five years old.

10. A second image I reviewed depicted an underage female, approximately four to five years old, touching the erect penis of an adult male.

C. Legal Process Served on AT&T to Determine Subscriber Information

11. On October 18, 2018, I served an ICE summons on AT&T, the provider that was named in Cyber Tipline Report, ID# 29684450, for subscriber data associated with SUSPECT IP ADDRESS. SUSPECT IP ADDRESS was listed on the Cyber Tipline Report, ID# 29684450. The subscriber data for SUSPECT IP ADDRESS was as follows:

a. Name: David LEWIS

b. Service and Billing Address: 8550 Commonwealth Ave., Apt. 415, Buena Park, California 90621

c. Activation Date: February 6, 2018

d. Home Phone: (714) 860-6764

12. Based on the results from the information provided to NCMEC by Google, which were provided to me via NCMEC Tipline Report, ID# 29684450, and the IP address subscriber information results for SUSPECT IP ADDRESS, the IP address used to upload the two sexually explicit images of child pornography comes back to the SUBJECT PREMISES.

D. Lewis's Connection to SUBJECT PREMISES

13. On October 9, 2018, I conducted a CLEAR database query and learned that according to Experian, Equifax, and Transunion credit information, as well as utility listings, David A. LEWIS, date of birth December 8, 1968, currently resides at the SUBJECT PREMISES.

14. On October 9, 2018, I checked California Department of Motor Vehicles ("DMV") records associated with LEWIS by inputting LEWIS's name and California driver's license number. The DMV records: (1) contained a photograph of LEWIS; (2) provided LEWIS's sole registered vehicle as a 1999 Ford, California license plate 5V29443, and (3) revealed that LEWIS, date of birth December 8, 1968, resides at the SUBJECT PREMISES.

15. On October 9, 2018, I conducted a query of LEWIS's name and date of birth in the California Sex and Arson Registration ("CSAR") law enforcement database. The query revealed that LEWIS is in fact a registered sex offender. LEWIS registered as a sex offender with the Buena Park Police Department ("BPPD") on December 8, 2017, and provided his address as the SUBJECT PREMISES. LEWIS also provided BPPD with a copy of his driver's license for verification.

16. On October 10, 2018, at approximately 4:00 p.m., I went to the area of the Fullerton Court Apartment Homes where the SUBJECT PREMISES is located, and took pictures of the SUBJECT PREMISES and also saw a beige colored Ford F-350 truck, California license plate 5V29443, backed into a parking spot near the SUBJECTS PREMISES. California Department of Motor Vehicle (DMV) records reveal that LEWIS is the registered owner of this vehicle.

17. On October 11, 2018 at approximately 8:50 a.m., I again went to the area of the SUBJECT PREMISES. Upon arriving at the apartment complex, LEWIS's vehicle (1999 Ford F-350 truck, California license plate 5V29443) was not located at the SUBJECTS PREMISES. At approximately 9:10 a.m., I saw LEWIS's Ford truck enter the apartment complex and back into the same parking spot that LEWIS's truck was parked in the previous afternoon. I also saw a man in a red shirt and dark pants get out of the Ford truck and walk in the direction of the SUBJECTS PREMISES. Based on my review of LEWIS's California Driver's License photo (number C6299771), I believed the driver of the Ford truck to be LEWIS.

E. National Crime Information Center (NCIC) Criminal History Database Query for David LEWIS, DOB xx/xx/1968

18. On or about October 18, 2018, I conducted a search of the National Crime Information Center ("NCIC") database for the criminal history of David LEWIS (Date of Birth: xx/xx/1968), which returned the following results:

a. On or about December 7, 2010, LEWIS registered as a sex offender with the Cypress Police Department for a prior criminal conviction on February 13, 2007, for a violation of State of California Penal Code Section 311.11(a) (Possession/control of obscene matter depicting a minor engaging in or simulating sexual conduct).

b. On or about December 8, 2017, LEWIS contacted BPPD to continue his pre-existing sex offender registration which he originally filed in 2010.

c. On October 18, 2018, I went to BPPD to obtain information regarding LEWIS's sex offender registration. During my review of CSAR information related to LEWIS, I saw LEWIS's cell phone number listed as (714) 860-6764, which is the same number listed on LEWIS's AT&T subscriber information, as provided by AT&T. CSAR information listed LEWIS's address as SUBJECTS PREMISES. CSAR information also included LEWIS's driver's license number and other identifiers, as well as a picture of LEWIS, which upon review confirms him as the same person depicted on his California driver's license photo.

F. Characteristics Common to Individuals Who Receive, Possess, or Access with Intent to View Child Pornography

19. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement agents and officers with whom I have had discussions, I know there are certain characteristics common to individuals who receive, possess,

and/or access the internet with the intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child

erotica, and videotapes for many years. In this particular case, the person with a sexual interest in children at the SUBJECT PREMISES accessed the google website for the purpose of viewing child pornography and uploaded two sexually explicit images.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do

their sexually explicit material, and often maintain lists of names, addresses (including e-mail addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if LEWIS uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as well as any garage or storage unit on site belonging to LEWIS, and LEWIS's vehicle, as set forth in **Attachment A**.

h. Such individuals often use a proxy server, a VPN, or a Tor to act as a relay to conceal their IP address thus their physical location, especially when purchasing something illegal such as child pornography.

20. Based on the following, I believe that the user of the computer(s) or other electronic devices residing at the SUBJECT PREMISES likely displays characteristics common to individuals who are in receipt of, or access with intent to view child pornography. For example, the target of this investigation searched for, viewed, and accessed and potentially saved child pornographic images on March 6, 2018. Based on this fact, I believe the user has saved and stored these photographs at the

SUBJECT PREMISES, along with other illegal child pornographic related content.

VII. BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

21. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers serve four functions in connection with child pornography; production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "Wi-Fi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can

therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices, which plug into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Individuals can easily store, carry or conceal media storage devices on their persons. Individuals also often carry Smartphones and/or mobile phones.

e. The internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the internet. Even in

cases where an individual uses online storage, however, law enforcement can find evidence of child pornography on the user's computer, smartphone or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information such as the traces of the path of an electronic communication may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information exists indefinitely until overwritten by other data.

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

22. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related

communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. As a result,

a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.[1] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not

[1] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For

example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed.

A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

23. As discussed herein, based on my training and experience I believe that digital devices will be found during the search. I believe that the target most likely also possesses a cell phone, and that it is very common for cell phones to have one or more biometric features for the unlocking of such devices.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the

relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes

open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features

including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

24. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

25. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has

activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

26. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features (such as with Touch ID devices, which can be registered with up to five fingerprints), and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require LEWIS to unlock a device found at the SUBJECT PREMISES using biometric features in the same manner as discussed in the following paragraph, as long

as LEWIS is reasonably believed by law enforcement to be a user of the device.

27. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to biometric sensor-enabled devices reasonably believed by law enforcement to be used by LEWIS that is (a) located at the SUBJECT PREMISES and (b) falls within the scope of the warrant: (1) compel the use of LEWIS's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of LEWIS with his eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

28. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

//

//

//

IX. CONCLUSION

29. For all the reasons described above, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(d) (advertisement of child pornography), 18 U.S.C. § 2252A(a)(2) (receipt and distribution of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography), as described in **Attachment B** to this affidavit, will be found in a search of the SUBJECT PREMISES, which is further described above and in **Attachment A** of this affidavit.

ARON KLAFF,
Special Agent,
Homeland Security
Investigations

Subscribed to and sworn before me

October ____, 2018.

HONORABLE EDWARD INFANTE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is the property located at 8550 Commonwealth Ave., Apt. 415, Buena Park, California, 90621 (the "SUBJECT PREMISES"). The SUBJECT PREMISES is an apartment unit on the second story of a two-story multi-family apartment complex with the front door facing east. The exterior color of the apartment building is beige in color and has a dark brown front door. The front door has dull gold-colored numbers on it that read "415". While facing the front door, there is one rectangular aluminum window for Apt. 415 to the right of the front door. Just below the window lies an air conditioning unit which is affixed onto the exterior wall of the building. The front of the apartment complex has a brown sign with off-white letters with the apartment complex's information as follows: Fullerton Court Apartment Homes (714) 670-1308, 8550 Commonwealth Ave.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 2251(d) (advertisement of child pornography), 18 U.S.C. § 2252A(a)(2) (receipt and distribution of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography), namely:

a. Child pornography, as defined in 18 U.S.C. § 2256(8).

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8), including documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, ordering, requesting, or trading of child pornography, or documents that refer to a transaction of any kind involving child pornography.

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, ordering, requesting, or trading of child pornography, or involved in a transaction of any kind involving child pornography, as defined in 18 U.S.C. § 2256(8).

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

e. Any and all records, documents, programs, applications, materials, or items that are sexually arousing to individuals who are interested in minors, but that are not in and of themselves obscene or that do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques relating to child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to peer-to-peer file-sharing software.

g. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to accounts with any Internet Service Provider.

h. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of 8550 Commonwealth Ave., Apt. 415, Buena Park, California 90621 (the "SUBJECT PREMISES").

i. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

j. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and

connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without first obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to

determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. During the execution of this search warrant, the law enforcement personnel are authorized to: (1) depress the fingerprints and/or thumbprints of David Andrew LEWIS ("LEWIS"); and (2) hold the device in front of the face of LEWIS with his eyes open to activate the facial-, iris-, or retina-recognition feature, if LEWIS is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not

apply to any search of digital devices pursuant to any other court order.